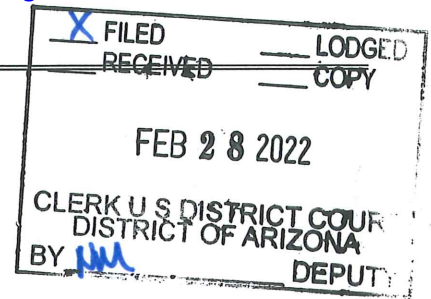


Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of

(Briefly Describe the property to be searched or identify the person by name and address)

The residence, garage and vehicles located at 3188
Robert Way, Yuma, Arizona 85365-2904

Case No. 22-1314MB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of Arizona.
(identify the person or describe the property to be searched and give its location):

As further described in Attachment A.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

As set forth in Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before 3/14/2022.
(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any United States Magistrate Judge on criminal duty in the district of Arizona.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for days (not to exceed 30)
☐ until, the facts justifying, the later specific date of .

Date and time issued: 2/28/2022 at 2:48 pmCity and State: Yuma, Arizona

Judge's signature

Honorable James F. Metcalf, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A**DESCRIPTION OF THE PERSON, PROPERTY, AND ITEMS****TO BE SEARCHED****PROPERTY:**

The residence located at 3188 S. Robert Way, Yuma, Arizona 85365-2904, which is a condominium. The house is tan with a stucco exterior and has a pitched roof with brown, tile shingles. The residence has a two-car garage with a white garage door. The front of the house faces east. The front door of the house is behind the garage and is not visible from the street. The numbers 3188 are displayed above the garage door in black three (3) inch numbers. The rear of the house faces west, and a cinderblock wall encloses the back yard. To the north and slightly separated from the residence, is 3182. To the south and sharing a wall with the residence, is 3190. I have verified that HERRERA and his wife reside at the 3188 S. Robert Way, Yuma, Arizona 85365-2904. I have determined that there is one vehicle (a associated with the residence and that is always parked in the garage. Because people often keep electronic devices of the type to be seized in their personal vehicles (either purposefully or accidentally), I am including the garage and the black 2016 Hyundai Accent bearing Arizona license plate CKJ6346 (vin# KMHCT4AE6GU113746) parked inside the garage as part of the property to be searched.

ITEMS:

Search for all items listed within ATTACHMENT B.

ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

1
2
3 1. Images of child pornography and files containing images of child pornography in any form
4 wherever it may be stored or found including:

5 a. Any computer, computer system and related peripherals; cellular phones,
6 personal digital assistants, tapes, cassettes, cartridges, streaming tape, commercial software and
7 hardware, computer disks, disk drives, monitors, computer printers, scanners, modems, tape
8 drives, disk applications programs, data disks, system disk operating systems, magnetic media
9 floppy disks, hardware and software operating manuals, tape systems and hard drive and other
10 computer-related operation equipment, firewalls, switches, hubs, wireless access points, gaming
11 consoles, web cameras, uninterrupted power supplies, hardware device power supplies, tape
12 backup drives, digital video recorders, undeveloped photographic film, slides, and other visual
13 depictions of such Graphic Interchange formats (including JPG, GIF, TIP AVI, and MPEG), and
14 any electronic data storage devices including, hardware, software, diskettes, backup tapes, CD-
15 ROMS, DVD, flash memory devices, and other storage mediums; any input/output peripheral
16 devices, including computer passwords and data security devices an computer-related
17 documentation, and any hardware/software manuals related to or used to: visually depict child
18 pornography; contain information pertaining to the interest in child pornography; distribute,
19 receive, or possess child pornography;

20 b. Books and magazines containing child pornography;

21 c. Originals, copies, and negatives of visual depictions of child pornography; and

22 d. Motion pictures, films, videos, and other recordings of visual depictions of child
23
24
25
26
27
28

1 pornography.

2 2. Information, correspondence, records, documents or other materials pertaining to the
3 possession, receipt or distribution of child pornography that were transmitted or received using
4 a computer, some other facility or means of interstate or foreign commerce, or common carrier
5 of the U.S. mail including:
6

7 a. Envelopes, letters and other correspondence including electronic mail, chat logs,
8 and electronic messages, establishing possession, access to, or transmission through interstate or
9 foreign commerce, including by U.S. mail or by computer, of child pornography;
10

11 b. Books, ledgers and records bearing on the productions, reproduction, receipt,
12 shipment, orders, requests, trades, purchases or transactions of any kind involving the
13 transmission through interstate or foreign commerce, including by U.S. mail or by computer of
14 child pornography;
15

16 c. Records, documents, or materials, including any and all address books, mailing
17 lists, supplier lists, mailing address labels, and documents and records pertaining to the
18 preparation, purchase and acquisition of names or lists of names to be used in connections with
19 the purchase, sale, trade or transmission of child pornography, through interstate commerce
20 including by U.S. mail or by computer;
21

22 d. Records, documents or materials, including address books, names and lists of
23 names and addresses of minors visually depicted in child pornography;
24

25 e. Records of Internet usage, including user names and e-mail addresses and
26 identities assumed for the purposes of communication on the Internet to purchase, sell, trade,
27 transmit or acquire child pornography. These records may include ISP records, i.e., billing and
28

1 subscriber records, chat room logs, e-mail messages and include electronic files in a computer
2 and on other data storage mediums, including CDs or DVDs.

3 3. Credit card information, which evidences ownership or use of the computer equipment,
4 found in the above residence, including payment for Internet access and computers or electronic
5 media or other storage devices, disks, CD-ROMS, or similar containers for electronic evidence.
6

7 4. Records evidencing occupancy or ownership of the premises described above, including
8 utility and telephone bills, mail, envelopes or addressed correspondence.
9

10 5. Records or other items, which evidence ownership or use of computer equipment, found
11 in the above residence, including sales receipts, bills for Internet access and handwritten notes.
12

13 6. Any computer hard drive or other electronic media ("COMPUTER"), physically located
14 at the residence or virtually connected to any computer within the residence, found to contain
15 information otherwise called for by this warrant:

16 a. Evidence of who used, owned, or controlled the COMPUTER at the time the things
17 described in this warrant were created, edited, or deleted, such as logs, registry entries, saved
18 usernames and passwords, documents, and browsing history;
19

20 b. Evidence of software that would allow others to control the COMPUTER, such as
21 viruses, Trojan horses, and other forms of malicious software;
22

23 c. Evidence of the lack of such malicious software;

24 d. Evidence of the attachment to the COMPUTER of other storage devices, disks,
25 CD-ROMS, or similar containers for electronic evidence;

26 e. Evidence of the times the COMPUTER was used;

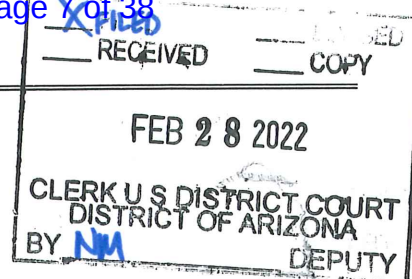
27 f. Passwords, encryption keys, and other access devices that may be necessary to
28

access the COMPUTER.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of

(Briefly Describe the property to be searched or identify the person by name and address)

The residence, garage and vehicles located at 3188
Robert Way, Yuma, Arizona 85365-2904

Case No.

22-1314 MB

APPLICATION AND AFFIDAVIT FOR A SEARCH AND SEIZURE WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

As further described in Attachment A.

Located in the District of Arizona, there is now concealed (*identify the person or describe the property to be seized*):

The person or property to be searched, described above, is believed to conceal (*identify the person or describe the property to be seized*):

As set forth in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code/Section	Offense Description
Title 18 U.S.C. 2252	Activities Relating to Material Involving the Sexual Exploitation of Minors
Title 18 U.S.C. 2252A	Relating to Material Constituting or Containing Child Pornography

The application is based on these facts:

The Affidavit of Special Agent Benjamin Sumner is incorporated herein by reference.

- ☐ Continued on the attached sheet.
☐ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA Louie UhlLouie Uhl

BENJAMIN A SUMNER

Digitally signed by BENJAMIN A SUMNER
Date: 2022.02.25 21:38:10 -07'00'

Applicant's Signature

SA Benjamin Sumner, HSI

Applicant's printed name and title

Subscribed and sworn telephonically before me.

Date: 2/28/2022

Judge's signature

City and State: Yuma, Arizona

Honorable James F. Metcalf, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A**DESCRIPTION OF THE PERSON, PROPERTY, AND ITEMS****TO BE SEARCHED****PROPERTY:**

The residence located at 3188 S. Robert Way, Yuma, Arizona 85365-2904, which is a condominium. The house is tan with a stucco exterior and has a pitched roof with brown, tile shingles. The residence has a two-car garage with a white garage door. The front of the house faces east. The front door of the house is behind the garage and is not visible from the street. The numbers 3188 are displayed above the garage door in black three (3) inch numbers. The rear of the house faces west, and a cinderblock wall encloses the back yard. To the north and slightly separated from the residence, is 3182. To the south and sharing a wall with the residence, is 3190. I have verified that HERRERA and his wife reside at the 3188 S. Robert Way, Yuma, Arizona 85365-2904. I have determined that there is one vehicle (a associated with the residence and that is always parked in the garage. Because people often keep electronic devices of the type to be seized in their personal vehicles (either purposefully or accidentally), I am including the garage and the black 2016 Hyundai Accent bearing Arizona license plate CKJ6346 (vin# KMHCT4AE6GU113746) parked inside the garage as part of the property to be searched.

ITEMS:

Search for all items listed within ATTACHMENT B.

ATTACHMENT B**ITEMS TO BE SEARCHED AND SEIZED**

1
2
3 1. Images of child pornography and files containing images of child pornography in any form
4 wherever it may be stored or found including:

5 a. Any computer, computer system and related peripherals; cellular phones,
6 personal digital assistants, tapes, cassettes, cartridges, streaming tape, commercial software and
7 hardware, computer disks, disk drives, monitors, computer printers, scanners, modems, tape
8 drives, disk applications programs, data disks, system disk operating systems, magnetic media
9 floppy disks, hardware and software operating manuals, tape systems and hard drive and other
10 computer-related operation equipment, firewalls, switches, hubs, wireless access points, gaming
11 consoles, web cameras, uninterrupted power supplies, hardware device power supplies, tape
12 backup drives, digital video recorders, undeveloped photographic film, slides, and other visual
13 depictions of such Graphic Interchange formats (including JPG, GIF, TIP AVI, and MPEG), and
14 any electronic data storage devices including, hardware, software, diskettes, backup tapes, CD-
15 ROMS, DVD, flash memory devices, and other storage mediums; any input/output peripheral
16 devices, including computer passwords and data security devices an computer-related
17 documentation, and any hardware/software manuals related to or used to: visually depict child
18 pornography; contain information pertaining to the interest in child pornography; distribute,
19 receive, or possess child pornography;

20 b. Books and magazines containing child pornography;

21 c. Originals, copies, and negatives of visual depictions of child pornography; and

22 d. Motion pictures, films, videos, and other recordings of visual depictions of child
23
24
25
26
27
28

1 pornography.

2 2. Information, correspondence, records, documents or other materials pertaining to the
3 possession, receipt or distribution of child pornography that were transmitted or received using
4 a computer, some other facility or means of interstate or foreign commerce, or common carrier
5 of the U.S. mail including:
6

7 a. Envelopes, letters and other correspondence including electronic mail, chat logs,
8 and electronic messages, establishing possession, access to, or transmission through interstate or
9 foreign commerce, including by U.S. mail or by computer, of child pornography;
10

11 b. Books, ledgers and records bearing on the productions, reproduction, receipt,
12 shipment, orders, requests, trades, purchases or transactions of any kind involving the
13 transmission through interstate or foreign commerce, including by U.S. mail or by computer of
14 child pornography;
15

16 c. Records, documents, or materials, including any and all address books, mailing
17 lists, supplier lists, mailing address labels, and documents and records pertaining to the
18 preparation, purchase and acquisition of names or lists of names to be used in connections with
19 the purchase, sale, trade or transmission of child pornography, through interstate commerce
20 including by U.S. mail or by computer;
21

22 d. Records, documents or materials, including address books, names and lists of
23 names and addresses of minors visually depicted in child pornography;
24

25 e. Records of Internet usage, including user names and e-mail addresses and
26 identities assumed for the purposes of communication on the Internet to purchase, sell, trade,
27 transmit or acquire child pornography. These records may include ISP records, i.e., billing and
28

1 subscriber records, chat room logs, e-mail messages and include electronic files in a computer
2 and on other data storage mediums, including CDs or DVDs.

3 3. Credit card information, which evidences ownership or use of the computer equipment,
4 found in the above residence, including payment for Internet access and computers or electronic
5 media or other storage devices, disks, CD-ROMS, or similar containers for electronic evidence.
6

7 4. Records evidencing occupancy or ownership of the premises described above, including
8 utility and telephone bills, mail, envelopes or addressed correspondence.
9

10 5. Records or other items, which evidence ownership or use of computer equipment, found
11 in the above residence, including sales receipts, bills for Internet access and handwritten notes.
12

13 6. Any computer hard drive or other electronic media ("COMPUTER"), physically located
14 at the residence or virtually connected to any computer within the residence, found to contain
15 information otherwise called for by this warrant:

16 a. Evidence of who used, owned, or controlled the COMPUTER at the time the things
17 described in this warrant were created, edited, or deleted, such as logs, registry entries, saved
18 usernames and passwords, documents, and browsing history;
19

20 b. Evidence of software that would allow others to control the COMPUTER, such as
21 viruses, Trojan horses, and other forms of malicious software;
22

23 c. Evidence of the lack of such malicious software;

24 d. Evidence of the attachment to the COMPUTER of other storage devices, disks,
25 CD-ROMS, or similar containers for electronic evidence;

26 e. Evidence of the times the COMPUTER was used;

27 f. Passwords, encryption keys, and other access devices that may be necessary to
28

access the COMPUTER.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Benjamin Sumner, Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows, to wit:

INTRODUCTION

The facts of this case, as more fully detailed herein; specifically in paragraphs 16 through 18, are that on or about November 5, 2020, the United States Customs and Border Protection (CBP) Office of Professional Responsibility (OPR) referred this case to HSI Yuma after an applicant for a position, Carlos HERRERA, then an active duty United States Marine, stationed at Marine Corps Air Station (MCAS) Yuma, in Yuma, Arizona, within the District of Arizona, made admissions concerning child pornography during a pre-employment polygraph examination, in Yuma, Arizona, within the District of Arizona. During a consensual search of HERRERA's iPhone a pornographic image of a prepubescent female was discovered. Based on the information in this warrant, I am requesting that the Court issue a warrant to search 3188 S. Robert Way Yuma, Arizona 85365-2904, to locate child pornography and conclusively identify the individual(s) possessing and transmitting child pornography.

PRELIMINARY BACKGROUND INFORMATION

1. I am a Special Agent ("SA") with the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) and have been so employed since October 2018. I am currently assigned to the Public Safety Group. I have received training regarding the investigation of cases involving the sexual exploitation of children and the trafficking of children. During my employment in law enforcement, I have written and/or participated in the execution of multiple search warrants. The statements contained in this Affidavit are based on

1 my experience and background as a Special Agent and on information provided by other law
2 enforcement agents.

3 2. The purpose of this application is to seize evidence, more particularly described in
4 Attachment B, of violations of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), which make it a crime
5 to distribute and receive child pornography; violations of 18 U.S.C. §§ 2252(a)(1) and
6 2252A(a)(1), which make it a crime to transport or ship child pornography in interstate or foreign
7 commerce; and violations of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which makes it a
8 crime to possess, or knowingly access with intent to view, child pornography.
9

10 3. Because this Affidavit is being submitted for the limited purpose of securing a search
11 warrant, I have not included every fact known to me concerning this investigation. I have set
12 forth only those facts that are necessary to establish probable cause to believe that evidence of
13 violations of 18 U.S.C. §§ 2252 and 2252A is located at 3188 Robert Way, Yuma, Arizona
14 85365 ("SUBJECT PREMISES"), more particularly described in Attachment A, and within a
15 mobile device such as computer, and related peripherals and computer media found at the
16 SUBJECT PREMISES.
17
18
19

20 DEFINITIONS

21 4. The following non-exhaustive list of definitions applies to this Affidavit and Attachments
22 A and B (collectively referred to as "warrant"):

23 a. "Child Pornography" is any visual depiction of sexually explicit conduct where (a) the
24 production of the visual depiction involved the use of a minor engaged in sexually explicit
25 conduct, (b) the visual depiction is a digital image, computer image, or computer-generated
26 image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct,
27 or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable
28

1 minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).

2 b. "Child Erotica" means materials or items that are sexually arousing to persons having a
3 sexual interest in minors, but that are not, in and of themselves, obscene or illegal. In contrast
4 to "child pornography," this material does not necessarily depict minors in sexually explicit
5 poses or positions. Some of the more common types of child erotica include photographs that
6 are not sexually explicit, drawings, sketches, fantasy writing, and diaries. See Kenneth V.
7 Lanning, Child Molesters: A Behavioral Analysis (2001) at 65. Federal courts have recognized
8 the evidentiary value of child erotica and its admissibility in child pornography cases. See
9 United States v. Cross, 928 F.2d 1030 (11th Cir. 1991) (testimony about persons deriving sexual
10 satisfaction from and collecting non-sexual photographs of children admissible to show intent
11 and explain actions of defendant); United States v. Riccardi, 258 F.Supp.2d 1212 (D. Kan., 2003)
12 (child erotica admissible under Federal Rule of Evidence 404(b) to show knowledge or intent).

13 c. "Visual depictions" include undeveloped film and videotape, and data stored on
14 computer disk or by electronic means, which is capable of conversion into a visual image. See
15 18 U.S.C. § 2256(5).

16 d. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

17 e. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including
18 genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex;
19 (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of
20 the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

21 f. "Computer" means "an electronic, magnetic, optical, electrochemical, or other high
22 speed data processing device performing logical or storage functions, and includes any data
23
24
25
26
27
28

1 storage facility or communications facility directly related to or operating in conjunction with
2 such device.” See 18 U.S.C. § 1030(e)(1).

3 g. “Computer hardware” consists of all equipment that can receive, capture, collect,
4 analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar
5 computer impulses or data. Computer hardware includes any data-processing devices
6 (including central processing units, internal and peripheral storage devices such as fixed disks,
7 external hard drives, floppy disk drives and diskettes, and other memory storage devices),
8 peripheral input/output devices (including keyboards, printers, video display monitors, and
9 related communications devices such as cables and connections), as well as any devices,
10 mechanisms, or parts that can be used to restrict access to computer hardware (including physical
11 keys and locks).

12 h. “Computer software” is digital information that can be interpreted by a computer and
13 any of its related components to direct the way they work. Computer software is stored in
14 electronic, magnetic or other digital form. It commonly includes programs to run operating
15 systems, applications and utilities.

16 i. “Computer-related documentation” consists of written, recorded, printed, or
17 electronically stored material that explains or illustrates how to configure or use computer
18 hardware, computer software or other related items.

19 j. “Computer passwords and data security devices” consist of information or items
20 designed to restrict access to or hide computer software, documentation or data. Data security
21 devices may consist of hardware, software or other programming code. A password (a string
22 of alphanumeric characters) usually operates a sort of digital key to “unlock” particular data
23
24
25
26
27
28

1 security devices. Data security hardware may include encryption devices, chips and circuit
2 boards. Data security software of digital code may include programming code that creates
3 “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data
4 security software or code may also encrypt, compress, hide or “booby-trap” protected data to
5 make it inaccessible or unusable, as well as reverse the progress to restore it.
6

7 k. “Internet Service Providers” (ISPs) are commercial organizations, which provide
8 individuals and businesses access to the Internet. ISPs provide a range of functions for their
9 customers including access to the Internet, web hosting, e-mail, remote storage and co-location
10 of computers and other communications equipment. ISPs can offer various means to access the
11 Internet, including telephone based dial-up, broadband based access via a digital subscriber line
12 (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically
13 charge a fee based upon the type of connection and volume of data, called bandwidth that the
14 connection supports. Many ISPs assign each subscriber an account name such as a user name
15 or screen name, an e-mail address, and an e-mail mailbox and the subscriber typically creates a
16 password for the account. By using a computer equipped with a telephone or cable modem, the
17 subscriber can establish communication with an ISP over a telephone line or through a cable
18 system, and can access the Internet by using his or her account name and password.
19
20
21

22 1. “ISP Records” are records maintained by ISPs pertaining to their subscribers (regardless
23 of whether those subscribers are individuals or entities). These records may include account
24 application information, subscriber and billing information, account access information (often
25 times in the form of log files), e-mail communications, information concerning content uploaded
26 and/or stored on or via the ISP’s servers and other information, which may be stored both in
27
28

1 computer data format and in written or printed record format. ISPs reserve and/or maintain
2 computer disk storage space on their computer system for their subscribers' use. This service
3 by ISPs allows for both temporary and long-term storage of electronic communications and
4 many other types of electronic data and files.

5
6 m. "Internet Protocol address" (IP address) refers to a unique number used by a computer
7 to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider
8 (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP
9 addresses might also be static, if an ISP assigns a user's computer a particular IP address that is
10 used each time the computer accesses the Internet.

11
12 n. The terms "records," "documents" and "materials" include all information recorded in
13 any form, visual or aural, and by any means, whether in hand-made form (including writings,
14 drawings, painting), photographic form (including microfilm, microfiche, prints, slides,
15 negatives, videotapes, motion pictures, photocopies), mechanical form (including phonograph
16 records, printing, typing) or electrical, electronic or magnetic form (including tape recordings,
17 cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard
18 disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media
19 Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators,
20 electronic dialers or electronic notebooks, as well as digital data files and printouts or readouts
21 from any magnetic, electrical or electronic storage device).

22
23 o. "Digital device" includes any electronic system or device capable of storing and/or
24 processing data in digital form, including the following: central processing units; laptop or
25 notebook computers; PDAs; wireless communication devices such as telephone paging devices,
26
27
28

1 beepers and mobile telephones; peripheral input/output devices such as keyboards, printers,
2 scanners, plotters, monitors and drives intended for removable media; related communications
3 devices such as modems, cables and connections; storage media such as hard disk drives, floppy
4 disks, compact disks, magnetic tapes and memory chips; and security devices.

5
6 p. "Image" or "copy" refers to an accurate reproduction of information contained on an
7 original physical item, independent of the electronic storage device. "Imaging" or "copying"
8 maintains contents, but attributes may change during the reproduction.

9
10 q. "Hash value" refers to a mathematical algorithm generated against data to produce a
11 numeric value that is representative of that data. A hash value may be run on media to find the
12 precise data from which the value was generated. Hash values cannot be used to find other data.

13
14 r. "Steganography" refers to the art and science of communicating in a way that hides the
15 existence of the communication. It is used to hide a file inside another. For example, a child
16 pornography image can be hidden inside another graphic image file, audio file or other file
17 format.

18
19 s. "Compressed file" refers to a file that has been reduced in size through a compression
20 algorithm to save disk space. The act of compressing a file will make it unreadable to most
21 programs until the file is uncompressed.

22
23 t. "Domain Name" refers to the common, easy to remember names associated with an
24 Internet Protocol address. For example, a domain name of www.usdoj.gov refers to the Internet
25 Protocol address of 98.145.194.24. Domain names are typically strings of alphanumeric
26 characters with each level delimited by a period. Each level, read backwards - from right to
27 left- further identifies parts of an organization. Examples of first level or top-level domains are
28

1 typically .com for commercial organizations, .gov for the governmental organizations, .org for
2 organizations, and .edu for educational organizations. Second level names will further identify
3 the organization. For example, usdoj.gov further identifies the United States governmental
4 agency to be the Department of Justice. Additional levels may exist as needed until each
5 machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web
6 server located at the United States Department of Justice, which is part of the United States
7 government.
8

9 u. "Log Files" are records automatically produced by computer programs to document
10 electronic events that occur on computers. Computer programs can record a wide range of
11 events including remote access, file transfers, logon/logoff times, and system errors. Logs are
12 often named based on the types of information they contain. For example, web logs contain
13 specific information about when a website was accessed by remote computers; access logs list
14 specific information about when a computer was accessed from a remote location; and file
15 transfer logs list detailed information concerning files that are remotely transferred.
16
17

18 v. "Hyperlink" refers to an item on a web page which, when selected, transfers the user
19 directly to another location in a hypertext document or to some other web page.
20

21 w. "Website" consists of textual pages of information and associated graphic images. The
22 textual information is stored in a specific format known as Hyper-Text Mark-up Language
23 (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport
24 Protocol (HTTP).
25

26 x. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique
27 address for a file that is accessible on the Internet. For example, a common way to get to a
28

1 website is to enter the URL of the website's home page file in the Web browser's address line.
2 Additionally, any file within that website can be specified with a URL. The URL contains the
3 name of the protocol to be used to access the file resource, a domain name that identifies a
4 specific computer on the Internet, and a pathname, a hierarchical description that specifies the
5 location of a file in that computer.
6

7 **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

8 **AND ONLINE CHILD EXPLOITATION**

9
10 5. Based upon my knowledge, training and experience in online child exploitation and child
11 pornography investigations, as well as the experience and training of other law enforcement
12 officers with whom I have had discussions, I have learned the following:

13 a. Computers and computer technology have revolutionized the way in which child
14 pornography is produced, distributed, stored and communicated. Individuals can transfer
15 photographs or videos from a camera onto a computer-readable format with a variety of devices,
16 including scanners, memory card readers, or directly from digital cameras. The capability of a
17 computer to store images in digital form makes the computer itself an ideal repository for child
18 pornography. As explained further below, the storage capacity of electronic media used in
19 home computers has increased tremendously within the last several years. These drives can
20 store extreme amounts of visual images at very high resolution. Modems then allow computers
21 to connect to another computer through the use of telephone, cable, or wireless connection.
22 Electronic contact can be made to literally millions of computers around the world.
23

24 b. The Internet, the World Wide Web and other Internet components afford individuals
25 many different, and relatively secure and anonymous, venues for obtaining, viewing and trading
26
27
28

1 child pornography or for communicating with others to do so or to entice children.

2 Individuals can use online resources to retrieve, store and share child pornography, including
3 services offered by Internet Portals such as Google, America Online (AOL), Yahoo! and
4 Hotmail, among others. Online services allow a user to set up an account providing e-mail and
5 instant messaging services, as well as electronic storage of computer files in any variety of
6 formats. A user can set up an online storage account from any computer with access to the
7 Internet. Evidence of such online storage of child pornography is often found on the user's
8 computer. And even in cases where online storage is used, evidence of child pornography can
9 be found on the user's computer in most cases.
10
11

12 c. As is the case with most digital technology, computer communications can be saved or
13 stored on hardware and computer storage media used for these purposes. Storing this
14 information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the
15 location of one's favorite websites in, for example, "bookmarked" files. However, digital
16 information can also be retained unintentionally, e.g., traces of the path of an electronic
17 communication may be automatically stored in many places (e.g., temporary files or ISP client
18 software, among others). In addition to electronic communications, a computer user's Internet
19 activities generally leave traces or "footprints" in the web cache and history files of the browser
20 used. Such information is often maintained for very long periods of time until overwritten by
21 other data.
22
23
24

25 d. The interaction between software applications and the computer operating systems often
26 results in material obtained from the Internet being stored multiple times, and even in different
27 locations, on a computer hard drive without the user's knowledge. Even if the computer user is
28

1 sophisticated and understands this automatic storage of information on his/her computer's hard
2 drive, attempts at deleting the material often fail because the material may be automatically
3 stored multiple times and in multiple locations within the computer media. As a result, digital
4 data that may have evidentiary value to this investigation could exist in the user's computer
5 media despite, and long after, attempts at deleting it. A thorough search of this media could
6 uncover evidence of receipt, distribution and possession of child pornography.
7

8 e. Data that exists on a computer is particularly resilient to deletion. Computer files or
9 remnants of such files can be recovered months or even years after they have been downloaded
10 onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard
11 drive can be stored for years at little to no cost. Even when such files have been deleted, they
12 can be recovered months or years later using readily available forensic tools. When a person
13 "deletes" a file on a home computer, the data contained in the file does not actually disappear,
14 rather, the data remains on the hard drive until it is overwritten by new data. Therefore, deleted
15 files or remnants of deleted files, may reside in free space or slack space – that is, in space on
16 the hard drive that is not allocated to an active file or that is unused after a file has been allocated
17 to a set block of storage space for long periods of time before they are overwritten. In addition,
18 a computer's operating system may also keep a record of deleted data in a "swap" or "recovery"
19 file. Similarly, files that have been viewed via the Internet are automatically downloaded into
20 a temporary Internet directory or cache. The browser typically maintains a fixed amount of
21 hard drive space devoted to these files, and the files are only overwritten as they are replaced
22 with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic
23 file from a hard drive depends less on when the file was downloaded or viewed and more on a
24
25
26
27
28

1 particular user's operating system, storage capacity, and computer habits.

2 **BACKGROUND ON CELLULAR PHONE AND CHILD PORNOGRAPHY**

3 **AND ONLINE CHILD EXPLOITATION**

4
5 6. Based upon my knowledge, training and experience in online child exploitation and child
6 pornography investigations, as well as the experience and training of other law enforcement
7 officers with whom I have had discussions, I have learned the following:

8 a. Cellular telephones have revolutionized the way in which child pornography is
9 produced, distributed, stored and communicated as a commodity and a further tool of online
10 child exploitation.
11

12 b. A cellular telephone is a handheld wireless device used for voice and data
13 communication through radio signals. These telephones send signals through networks of
14 transmitter/receivers, enabling communication with other wireless telephones or traditional
15 "land line" telephones. A cellular telephone usually contains a "call log," which records the
16 telephone number, date, and time of calls made to and from the phone. In addition to enabling
17 voice communications, wireless telephones offer a broad range of capabilities. These
18 capabilities include: storing names and phone numbers in electronic "address books;" sending,
19 receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still
20 photographs and moving video; storing and playing back audio files; storing dates,
21 appointments, and other information on personal calendars; and accessing and downloading
22 information from the Internet. Cellular telephones may also include global positioning system
23 ("GPS") technology for determining the location of the device.
24
25
26

27 c. The capability of a cellular telephone to store images in digital form makes the cellular
28

1 telephone itself an ideal repository for child pornography. As explained further below, the
2 storage capacity of electronic media used in home cellular telephones has increased
3 tremendously within the last several years. These drives can store extreme amounts of visual
4 images at very high resolution.
5

6 d. The Internet, the World Wide Web and other Internet components afford individuals
7 many different and relatively secure and anonymous venues for obtaining, viewing and trading
8 child pornography or for communicating with others to do so or to entice children.
9

10 e. Individuals can use online resources to retrieve, store and share child pornography,
11 including services offered by Internet Portals such as Google, America Online (AOL), Yahoo!
12 and Hotmail, among others. Online services allow a user to set up an account providing e-mail
13 and instant messaging services, as well as electronic storage of cellular telephone files in any
14 variety of formats. A user can set up an online storage account from any cellular telephone with
15 access to the Internet. Evidence of such online storage of child pornography is often found on
16 the user's cellular telephone. And even in cases where online storage is used, evidence of child
17 pornography can be found on the user's cellular telephone in most cases.
18
19

20 f. The interaction between software applications and the cellular telephone operating
21 systems often results in material obtained from the Internet being stored multiple times, and even
22 in different locations, on a cellular telephone hard drive without the user's knowledge. Even if
23 the cellular telephone user is sophisticated and understands this automatic storage of information
24 on his/her cellular telephone's storage, attempts at deleting the material often fail because the
25 material may be automatically stored multiple times and in multiple locations within the cellular
26 telephone media. As a result, digital data that may have evidentiary value to this investigation
27
28

1 could exist in the user's cellular telephone media despite, and long after, attempts at deleting it.
2 A thorough search of this media could uncover evidence of receipt, distribution and possession
3 of child pornography.

4 **BACKGROUND ON PEER TO PEER FILE SHARING**

5
6 7. An increasingly common activity on the Internet is peer-to-peer file sharing (P2P). P2P
7 file sharing is a method of communication available to Internet users through the use of special
8 software. Computers linked together through the Internet using this software form a network
9 that allows for the sharing of digital files between users on the network. A user first obtains the
10 P2P software, which can be downloaded from the Internet. In general, P2P software allows the
11 user to designate file(s) on a computer to be shared with others worldwide running compatible
12 P2P software. A user looking to download files simply conducts a keyword search. The
13 results of the keyword search are displayed and the user then selects the file(s) that he/she wants
14 to download. The download of a file is achieved through a direct connection between the
15 computer requesting the file and the computer(s) hosting the file. Once a file has been
16 downloaded, it is stored in the area previously designated by the user and will remain there until
17 moved or deleted.

18
19 8. One of the advantages of some P2P file sharing programs is that multiple files may be
20 downloaded in parallel. This means that the user can download more than one file at a time.
21 In addition, a user may download parts of one file from more than one source computer at a time.
22 For example, a P2P user downloading an image file may actually receive parts of the image from
23 multiple computers. The advantage of this is that it speeds up the time it takes to download the
24 file. Often, however, a P2P user downloading an image file receives the entire image from one
25
26
27
28

1 computer.

2 9. A P2P file transfer is accomplished by reference to an Internet Protocol (IP) address. This
3 address, expressed as four groups of numbers separated by decimal points, is unique to a
4 particular computer during an online session. The IP address provides a unique location making
5 it possible for data to be transferred between computers. Software is available to identify the
6 IP address of the P2P computer sending the file and to identify if parts of the file came from one
7 or more IP addresses. Such software monitors and logs Internet and local network traffic. In
8 addition, most of the P2P software applications keep logs of each download event.
9

10 10. Even though P2P networks link together computers all over the world and users can
11 download files, it is not possible for one user to send or upload a file to another user through the
12 P2P network. The software is designed only to allow files to be downloaded that have been
13 selected. One does not have the ability to send files from his/her computer to another user's
14 computer or to download files from another user's computer without the other user's permission,
15 knowledge, and active participation.
16

17 11. The computers that are linked together to form a P2P network are located throughout the
18 world; therefore, the P2P network operates in interstate and foreign commerce. A person that
19 includes child pornography files in his/her "shared" folder is hosting child pornography and is
20 thereby promoting, presenting, and potentially distributing child pornography.
21

22 **BACKGROUND ON COMPUTERS AND EVIDENCE ASSESSMENT PROCESS IN**

23 **CHILD PORNOGRAPHY AND CHILD EXPLOITATION**

24 **INVESTIGATIONS**

25 12. Based upon my knowledge, training, and experience, as well as information related to me
26
27
28

1 by agents and others involved in the forensic examination of digital devices, I know that
2 segregating information before commencement of the review of digital evidence by the
3 examining agent is inconsistent with the evidence assessment process in child pornography and
4 online child exploitation investigations. This is true in part because the items to be searched
5 will not only contain child pornography but also will contain the identity of the user/possessor
6 of the child pornography as well as evidence as to the programs and software used to obtain the
7 child pornography, which may be located throughout the areas to be searched.
8

9
10 a. As further described in Attachment B, this warrant seeks permission to locate not
11 only computer files that might serve as direct evidence of the crimes described in the warrant,
12 but also for evidence that establishes how computers were used, the purpose of their use, and
13 who used them. Additionally, the warrant seeks information about the possible location of other
14 evidence.
15

16 b. As described above and in Attachment A, this application seeks permission to search
17 and seize certain records that might be found in the SUBJECT PREMISES, in whatever form
18 they are found. One form in which the records might be found is stored on a computer's hard
19 drive, or other electronic media. Some of these electronic records might take the form of files,
20 documents, and other data that is user-generated. Some of these electronic records, as explained
21 below, might take a form that becomes meaningful only upon forensic analysis.
22

23
24 c. Although some of the records called for by this affidavit might be found in the form
25 of user-generated documents (such as word processor, picture and movie files), computer hard
26 drives can contain other forms of electronic evidence that are not user-generated. In particular,
27 a computer hard drive may contain records of how a computer has been used, the purposes for
28

1 which it was used and who has used these records, as described further in the attachments. For
2 instance, based upon my knowledge, training and experience, as well as information related to
3 me by agents and others involved in the forensic examination of digital devices, I know the
4 following:

5
6 i. Data on the hard drive not currently associated with any file can provide
7 evidence of a file that was once on the hard drive but has since been deleted
8 or edited, or of a deleted portion of a file (such as a paragraph that has been
9 deleted from a word processing file).

10
11 ii. Virtual memory paging systems can leave traces of information on the
12 hard drive that show what tasks and processes the computer were recently in
13 use.

14
15 iii. Web browsers, e-mail programs and chat programs store configuration
16 information on the hard drive that can reveal information such as online
17 nicknames and passwords.

18
19 iv. Operating systems can record additional information, such as the
20 attachment of peripherals, the attachment of USB flash storage devices and
21 the times the computer was in use.

22
23 v. Computer file systems can record information about the dates files were
24 created and the sequence in which they were created. This information may
25 be evidence of a crime or indicate the existence and location of evidence in
26 other locations on the hard drive.

27
28 d. Further, in finding evidence of how a computer has been used, the purposes for which

1 it was used and who has used it, sometimes it is necessary to establish that a particular thing is
2 not present on a hard drive or that a particular person (in the case of a multi-user computer) was
3 not a user of the computer during the time(s) of the criminal activity. For instance, based upon
4 my knowledge, training and experience, as well as information related to me by agents and others
5 involved in the forensic examination of digital devices, I know that when a computer has more
6 than one user, files can contain information indicating the dates and times that files were created
7 as well as the sequence in which they were created, and, for example, by reviewing the Index.dat
8 files (a system file that keeps track of historical activity conducted in the Internet Explorer
9 application), whether a user accessed other information close in time to the file creation dates,
10 times and sequences so as to establish user identity and exclude others from computer usage
11 during times related to the criminal activity.
12

13
14
15 e. Evidence of how a digital device has been used, what it has been used for and who has
16 used it, may be the absence of particular data on a digital device and requires analysis of the
17 digital device as a whole to demonstrate the absence of particular data. Evidence of the absence
18 of particular data on a digital device is not segregable from the digital device.
19

20 f. The types of evidence described above may be direct evidence of a crime, indirect
21 evidence of a crime indicating the location of evidence or a space where evidence was once
22 located, contextual evidence identifying a computer user and contextual evidence excluding a
23 computer user. All of these types of evidence may indicate ownership, knowledge and intent.
24

25 g. This type of evidence is not “data” that can be segregated, that is, this type of data cannot
26 be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to
27 investigators. Rather, evidence of this type is a conclusion, based on a review of all available
28

1 facts and the application of knowledge about how a computer behaves and how computers are
2 used. Therefore, contextual information is necessary to understand the evidence described in
3 Attachment B also falls within the scope of the warrant.

4 **SEARCH METHODOLOGY TO BE EMPLOYED**

5
6 13. As noted within this search warrant, it would be extremely difficult, if not impossible to
7 conduct a thorough on-site review of all of the potential evidence in this case. Given these
8 constraints, the search methodology to be employed is as follows:

9
10 a. All computers, computer hardware and any form of electronic storage that could contain
11 evidence described in this warrant will be seized for an off-site search for evidence that is
12 described in the attachments of this warrant. It is anticipated that mirror copies or images of such
13 evidence will be made if the failure to do so could otherwise potentially alter the original
14 evidence.
15

16 b. Consistent with the information provided within this affidavit, contextual information
17 necessary to understand the evidence, to identify the user/possessor of the child pornography,
18 and to establish admissibility of the evidence in subsequent legal proceedings will also be sought
19 by investigative agents.
20

21 c. Additional techniques to be employed in analyzing the seized items will include (1)
22 surveying various file directories and the individual files they contain; (2) opening files to
23 determine their contents; (3) scanning storage areas, (4) performing key word searches through
24 all electronic storage areas to determine whether occurrences of language contained in such
25 storage areas exist that are likely to appear in the evidence described in this affidavit and its
26 attachments, and (5) performing any other data analysis techniques that may be necessary to
27
28

1 locate and retrieve the evidence described in this affidavit and its attachments.

2 14. Because it is expected that the computers, computer hardware and any form of electronic
3 storage media may constitute (1) instrumentality of the offense, (2) fruit of criminal activity, (3)
4 contraband, or (4) evidence otherwise unlawfully possessed, it is anticipated that such evidence
5 will not be returned to the owner and that it will be either forfeited or ultimately destroyed in
6 accordance with the law at the conclusion of the case.
7

8 a. Because of the large storage capacity as well as the possibility of hidden data within the
9 computers, computer hardware and any form of electronic storage media, it is anticipated that
10 there will be no way to ensure that contraband-free evidence could be returned to the
11 user/possessor of the computer, computer hardware or any form of electronic storage media,
12 without first wiping such evidence clean. Wiping the original evidence clean would mean that
13 the original evidence would be destroyed and thus, would be detrimental to the investigation and
14 prosecution of this case.
15
16

17 b. Further, because investigators cannot anticipate all potential defenses to the offenses in
18 this affidavit, and as such, cannot anticipate the significance of the evidence that has been
19 lawfully seized pursuant to this warrant, it is requested that all seized evidence be retained by
20 law enforcement until the conclusion of legal proceedings or until other order of the court.
21

22 c. If after careful inspection investigators determine that such computers, computer
23 hardware and electronic storage media do not contain (1) instrumentality of the offense, (2) fruit
24 of criminal activity, (3) contraband, (4) evidence otherwise unlawfully possessed, or (5) evidence
25 of the person who committed the offense and under what circumstances the offense was
26 committed, then such items seized will be returned.
27
28

CHARACTERISTICS OF INDIVIDUALS INVOLVED IN THE DISTRIBUTION OF
CHILD PORNOGRAPHY

15. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in the possession and distribution of child pornography. Those who possess and distribute child pornography:

a. May receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. May collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines,

1 correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many
2 years.

3 d. Often maintain their collections that are in a digital or electronic format in a safe, secure
4 and private environment, such as a computer and surrounding area. These collections are often
5 maintained for several years and are kept close by, usually at the individual's residence, to enable
6 the collector to view the collection, which is valued highly.

8 e. May correspond with and/or meet others to share information and materials; rarely
9 destroy correspondence from other child pornography distributors/collectors; conceal such
10 correspondence as they do their sexually explicit material; and often maintain lists of names,
11 addresses, and telephone numbers of individuals with whom they have been in contact and who
12 share the same interests in child pornography.

14 f. Prefer not to be without their child pornography for any prolonged time period. This
15 behavior has been documented by law enforcement officers involved in the investigation of child
16 pornography throughout the world.

18 DETAILS OF THE INVESTIGATION

19
20 16. On November 5, 2020, at approximately 1903 hours, Homeland Security Investigations
21 (HSI) Special Agents (SA) Fitzmorris and Sumner interviewed Carlos HERRERA regarding
22 admissions that HERRERA had made on and during a pre-employment polygraph examination,
23 in Yuma, Arizona. HERRERA was advised of his Fifth Amendment constitutional rights per
24 *Miranda*, both verbally and HERRERA confirmed that he understood those rights, waived them
25 and verified that he was willing to speak with the agents. HERRERA admitted that from June to
26 October of 2020, he had messaged approximately 20 underage females on Snapchat. Their ages,
27
28

1 he said, were between 13 and 15 years old. HERRERA stated that he had exchanged
2 pornographic pictures and videos with these females. He also stated that he had sent videos and
3 pictures of himself masturbating and exposing himself explicitly. HERRERA further stated that
4 he would ask these underage girls to send him nude pictures and videos of themselves naked and
5 masturbating. He also sent them pictures and videos of himself masturbating. HERRERA stated
6 that he told the underage girls that he was only 17. HERRERA stated that in the messages sent
7 by the females, they would often tell him their age. HERRERA consented both verbally and in
8 writing to search both of his cell phones (an iPhone 12 and an iPhone X).
9

10
11 17. On April 21, 2021, Special Agent Jay Fitzmorris gave Computer Forensics Agent (CFA)
12 Frank Salcedo the seized electronic evidence in the case against Carlos HERRERA for forensic
13 analysis along with a signed consent form. These items were: Apple iPhone X Smartphone. A
14 report was then generated documenting the information found in the extraction.
15

16 CFA Salcedo reviewed the contents of the report and an image of child exploitive material. The
17 files are as follows:
18

19 File Name: b7c2643a9bc95ed2ae1d21d53deabab536c1608

20 SHA1: 91A33877DB9619220F6293EDD4086375009FB7C3

21 Description: This is a picture of a MacBook laptop computer. On the screen is a close-up picture
22 of the vagina of a prepubescent female. The child has minimal pubic development. The child is
23 wearing a light blue t-shirt. She has minimal breast development. CFA Salcedo observed that
24 the image was sent to HERRERA's device from his wife. HERRERA's wife sent the image via
25 text and demanded to know why the image was on his laptop. She furthered texted HERRERA
26 that the image appeared when she opened his (HERRERA's) laptop.
27
28

18. Record checks revealed that HERRERA moved from his residence aboard MCAS Yuma to 3188 S. Robert Way, Yuma, AZ 85365. Further record checks revealed that HERRERA has a black 2016 Hyundai Accent bearing Arizona license plate CKJ6346 (vin# KMHCT4AE6GU113746).

On February 17th, 2022 at approximately 1955hrs, HSI Special Agents observed HERRERA driving a black Hyundai Accent into the garage at 3188 S. Robert Way, Yuma, AZ. HERRERA parked the vehicle and was seen exiting the vehicle after parking.

FORFEITURE

19. For Chapter 110 child pornography offenses, 18 U.S.C. §§ 2253 and 2254 provide the forfeiture authority. Section 2254 provides for civil forfeiture of the same property subject to criminal forfeiture in Section 2253, as requested in a criminal seizure warrant pursuant to 18 U.S.C. § 981.

20. Section 2253 provides, in relevant part:

(a) Property subject to criminal forfeiture -

(1) any visual depiction described in section 2251, 2251A, or 2252, 2252A, 2252B, or 2260 of this chapter, or any book, magazine, periodical, film, videotape, or other matter which contains any such visual depiction, which was produced, transported, mailed, shipped or received in violation of this chapter;

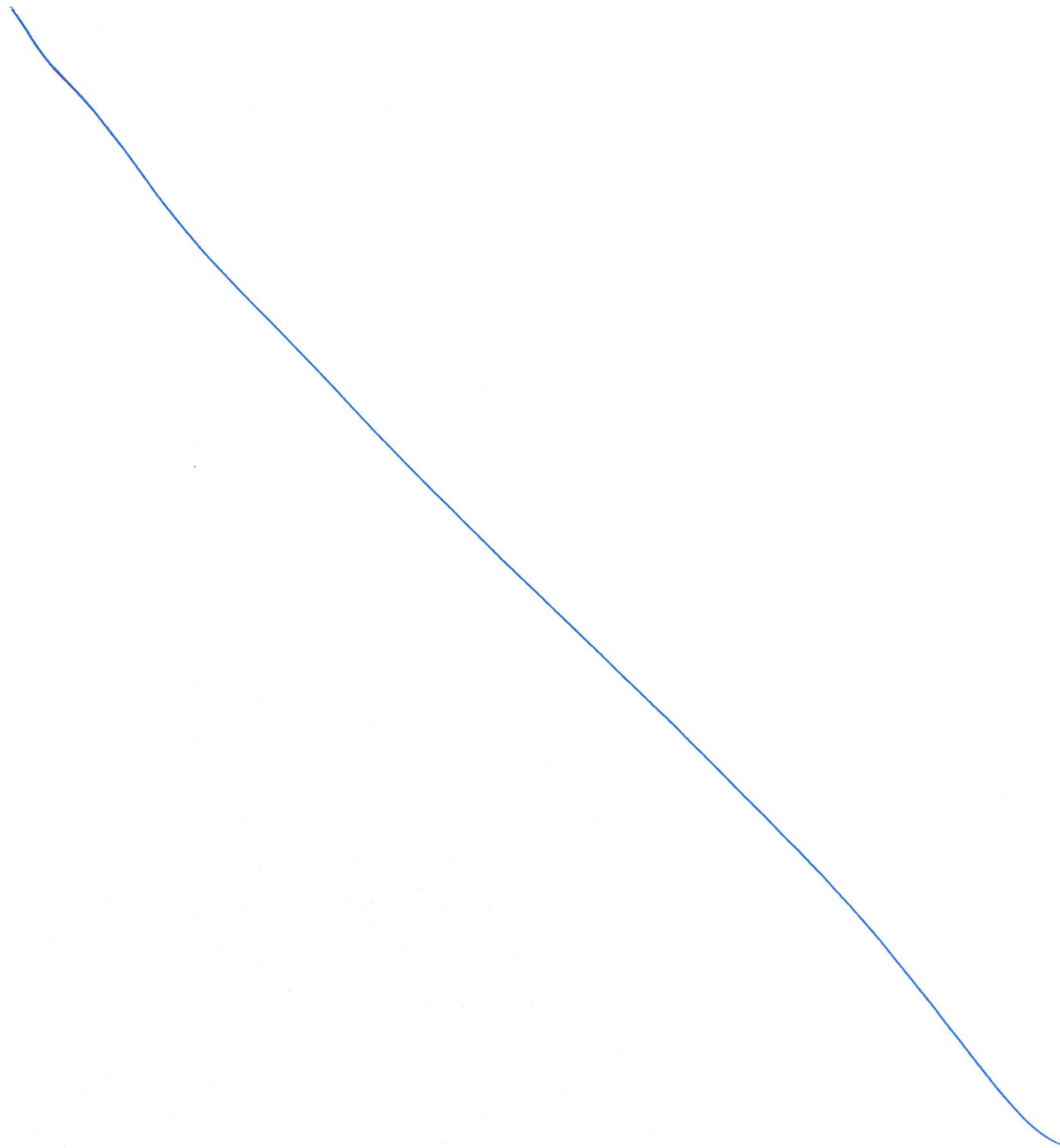
(2) any property, real or personal, constituting or traceable to gross profits or other proceeds obtained from such offense, and;

(3) any property, real or personal, used or intended to be used to commit or to

1 promote the commission of such offense or any property traceable to such
2 property.

3 21. Pursuant to these Rules, I request immediate forfeiture of any property, including items of
4 electronic evidence, which constitutes, contains, or was used to facilitate a crime involving child
5 pornography or online child exploitation.
6

7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



CONCLUSION

22. Based on the foregoing, I believe that there is probable cause that Carlos HERRERA has, stored on the SUBJECT PREMISES, electronic devices that he has utilized or is utilizing, in violation of Title 18 U.S.C. §§ 2252 and 2252A, which, among other things, makes it a federal crime for any person to produce, possess, receive, or distribute child pornography. I further believe that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, as more fully described in Attachment A.

Respectfully submitted,

Digitally signed by BENJAMIN A SUMNER

BENJAMIN A SUMNER Date: 2022.02.25 21:40:27 -07'00'

Benjamin Sumner

Special Agent

Homeland Security Investigations

Subscribed and sworn telephonically before me this 28th of February, 2022



Hon. James F. Metcalf
United States Magistrate Judge